



Bitcoin and The Blockchain

There is nothing more powerful than an idea whose time have come

Thursday, August 10, 2017

Chain Death Spiral - A Fatal Bitcoin Vulnerability

Back in Bitcoin history, when Argentinian millionaire Wences Caseres (Xapo, Paypal) came across Bitcoin he saw it as a potential solution to the periodic financial turmoil that totally wipes off the wealth of hard working Argentinians. In what I consider a very prudent act of due diligence, he paid a couple of hackers a sizable amount of money to hack and break the fledgling Bitcoin. Their conclusion was that it was unbreakable and that has remained true until today. The Bitcoin protocol has never been hacked. The vulnerabilities were the trusted infrastructure around it like the exchanges. The most memorable being MT Gox.

However on the 1st August 2017, Bitcoin main chain forked and a new coin Bitcoin Cash (BCH) came into existence. Some argue that it is closer to Satoshi's vision than the current Bitcoin (BTC) which separate the data portion from the address portion of the data structure. BTC became the main coin because it was supported by the majority of users, developers, Bitcoin businesses and miners in what is now known as the New York Agreement.

Chain Death Spiral. (CDS)

After Bitcoin fork on 1 August it became obvious that Bitcoin the protocol did have an inherent vulnerability. This was that if the chain loses mining power it will have to wait a full 2016 blocks before the difficulty can be adjusted to bring the block time back to the normal 10 minutes. This vulnerability was never considered or analysed because until now the miners had no choice but to keep mining on the Bitcoin chain. After the fork however, the whole landscape has changed. Miners have a choice and power to influence the fate of the chain they are mining on.

This was brought clearly into focus when the blocktime of the BCH fork went as high as 15 hours per block in the beginning. BCH however was designed with Emergency Difficulty Adjustment (EDA) which adjusted the difficulty even before the 2016 block adjustment period is up. Bitcoin (BTC) does not have this safety feature and cannot have one unless a hardfork is performed to include it.

A Chain Death Spiral occurs when the block time increases leading to some miners switching chain. As more miners leave the problem gets worse and a feedback loop results in the dreaded Chain Death Spiral.



Bitcoin (BTC) mempool been increasing since after the fork on 1st August. It is currently 52MB which means it will take 52 blocks to clear without any additional transactions. The record was in May 2017 when it reached 120MB. The whole community was in an uproar resulting in a move towards other competing coins for transacting.



Looking at the hashrate distribution and starting from the 6th August we get the following

Bitcoin And The Blockchain

• [Home](#)

Search This Blog

Translate

Powered by [Google Translate](#)

Blog Archive

- [2018](#) (8)
- ▼ [2017](#) (30)
 - [December](#) (3)
 - [November](#) (6)
 - [October](#) (3)
 - [September](#) (2)
 - ▼ [August](#) (10)
 - [Till Death Do Us Part - The Partening](#)
 - [Chain Death Spiral - Watch It In Real Time](#)
 - [Will The Real Bitcoin Please Stand Up. Please Stan...](#)
 - [A tale of Two Coins](#)
 - [Bitcoin Cash \(BCH\) Will Regain The Mantle To Be Bi...](#)
 - [Why is Bitcoin Price Rising. The Answer May Not Be...](#)
 - [Bitcoin Fork - Smoke Mirrors and A Game Of Poker](#)
 - [Chain Death Spiral - A Fatal Bitcoin Vulnerability...](#)
 - [BTC Is Dead, Long Live BTC - Updated and Explained...](#)
 - [BTC is dead - Long live BTC.](#)
- [July](#) (1)
- [June](#) (1)
- [March](#) (1)
- [February](#) (1)
- [January](#) (2)
- [2016](#) (5)
- [2015](#) (15)

About Me

Patrick

[G+](#) [Follow](#) 0

[View my complete profile](#)

Total Pageviews

165,121

Popular Posts

(Peta Hash)	BTC	BCH	TOTAL (Block Time)	BTC	BCH
6 August 2017	7473	143	7617	8.13	110
7 August 2017	6023	499	6612	10.28	22.15
8 August 2017	6637	551	7188	9.41	18.46
9 August 2017	6835	154	6989	8.78	62
10 August 2017	6200	541	6741	10.43	15

A picture is forming. Between 8 to 10 August roughly 400 petahashes moved out of BCH which triggered the EDA adjustments then move back in. In addition there was a loss of 200 Peta Hashes on the 9th August and a further 200 Peta Hashes loss on the 10th August.

The current BTC mempool is 50MB and blocktime is 10.28 minutes. There is clearly a development and it will get clearer today. Will the 400 Peta Hashes leave BCH again or will the hashing power on BTC decrease further. What happened to the 400 Peta Hashes missing since 8th August. The BTC chain cannot afford further loss of hashing power. Its' blocktime must come back to within 10 minutes and soon.

What is certain is that the current price of BTC is not justified with this inherent vulnerability, risk of the dreaded Chain Death Spiral. **Have investors totally abandoned any thought of immutable economic security and due diligence?** It is incredible how we lose sight of the risks when we bamboozled with riches, hype and misinformation through censorship.

It is other peoples' hard earned money and other peoples' investments. Even the possibility that this "black swan event" can happen must be addressed. It should never be censored speech.

Related Articles

BTC is Dead - Long Live BTC - [Here](#)

BTC is Dead - Long Live BTC Updated and Explained ELI5 - [Here](#)

Why is Bitcoin Price Rising - It May Not Be What You Think - [Here](#)

Bitcoin Fork - Smoke. Mirrors and a good game of Poker - [Here](#)

Bitcoin Cash Will regain the mantle to be Bitcoin - [Here](#)

Intelligent Comments

from [coinsinspace](#) via [/r/Bitcoin](#) sent 37 minutes ago

It's a textbook black swan because majority dismisses it automatically as impossible, yet it's unlikely but possible, and it would be very likely fatal.

If bitcoin was the only viable sha256 coin that would be a much smaller danger. In that case the mining power would have to completely disappear for long. It's much more likely if miners can switch, especially if the other chain is more profitable.

Once that happens there are several factors all accelerating the problem:
 (1) Mining rewards can only be spent after 100 blocks. Normally that's about 17 hours. If 90% of mining power disappeared that would take a week. So that's a strong incentive to mine something else (if available) in itself.
 (2) Bitcoin economy grinds to a halt, as transactions become increasingly impossible. This leads many people with coins on exchanges to buy other coins just to be able to transact, which lowers the price, making the alternative chain even more attractive for miners.

Which means that, as miners leave, the higher incentive the remaining miners have to also leave. In the event that almost all miners leave the difficulty reset never happens as chain dies.

Posted by [Patrick](#) at 4:15 PM



Labels: [bitcoin](#), [Bitcoin Cash](#), [Chain Death Spiral](#)

Chain Death Spiral - A Fatal Bitcoin Vulnerability

Back in Bitcoin history, when Argentinian millionaire Wences Caseres (Xapo, Paypal) came across Bitcoin he saw it as a potential solution ...

Bitcoin Cash (BCH) Will Regain The Mantle To Be Bitcoin

Here Is Why
 TOT BTC BCH
 BTC ...

Why is Bitcoin Price Rising. The Answer May Not Be What You Think.

Greater adoption especially in Japan. True. Higher prices leading to greater interest and media hype. True. Large investors and hedge fun...

Chain Death Spiral - Watch It In Real Time

You can watch the progress of the Chain Death Spiral in real time. Watch the progress of the orange line. Hover over it to follow the curr...

A tale of Two Coins

In 2005 Michael Burry discovered that the mortgage back securities that banks were selling to investors had included in them mortgages that...

33 comments



Add a comment as Rick De Jesus

Top comments

**Jason Williams** 5 days ago · Shared publicly

Thanks for sharing this information, Keep it up. Please Check Trading in Cryptocurrency with KZCash. <https://kzcash.kz/>

1

**shamir sam** 1 week ago · Shared publicly

Thanks for sharing this informative and interesting article with us. Follow the link to Join the first SEC-compliant **#ZENcoin** [href="https://preico.zenvideo.co/home">cryptocurrency](https://preico.zenvideo.co/home) crowdsale that features pricing usually only reserved for the rich or insiders, discounted pricing up to 50%

1 · Reply

**Dora Moore** 6 days ago · Shared publicly

if you want to know more about Bitcoin just visit Bitcoin Daily Post. Latest news covering everything about bitcoin and other cryptocurrencies. <http://www.bitcoindailypost.com>

1 · Reply

**PH Hema** 1 week ago · Shared publicly

Welcome to Alpha Obstructive Service! With the priority of quality, we provide heating, air conditioning, plumbing, blocking, disinfection, cesspool discharges and many other related to your home, apartment building or business throughout the prefecture of Attica. Our technicians are trained

Read more

1 · Reply

**Chris Moore** 6 months ago · Shared publicly

> Bitcoin Cash activated at block 478577. This means that the standard difficulty adjustment will take place at block 480593

That's not how it works. The difficulty adjustment happens at multiples of 2016, so the first one will be at block 479808.

+1 1 · Reply

**Patrick** 6 months ago

Think it starts from the last BTC adjustment block before the fork.

**Chris Moore** 6 months ago

You made it clear what you think in your article and that's why I corrected you. I thought maybe you would want to correct your mistake. Even if you don't, at least look into it rather than holding on to your false

[Read more](#)

**Shariar Porosh** 1 week ago · Shared publicly

Offers free cryptocurrency tools to use including live crypto prices, market cap, volume and calculator. <https://www.cryptocurrency.lu/>

1 · Reply

**Thomas Lundqvist** 6 months ago · Shared publicly

I think there might be a bit flawed reasoning here. If mining power leaves BTC, the remaining miners still get the same revenue since the earnings only depend on the difficulty, not the total hash rate (in the short run, before difficulty reductions). If this results in larger mempool, meaning higher fees, the remaining miners actually gain more. I see no reason to leave in such a

and remaining miners suddenly gain more. I see no reason to leave in such a case. Therefore, there will be no fatal spiral. Am I wrong?

1 · Reply

View all 4 replies



Thomas Lundqvist 6 months ago

No! I agree that confirmations will slow down but my hash power would still generate the same payments. Imagine if I had 50% of total hash power and the other 50% leave. Then, I will be the only one finding blocks every 20 min approx. So, still same pay. Before: 50% every 10 min. After: 100% every 20 min.



Allan Doensen 6 months ago

+**Thomas Lundqvist** If the blocks are full then that chain is still stuffed. If the blocks are not full, then I do not think this event will occur. So back to the blocksize debate.



Adrian van Wijk via Google+ 6 months ago · Shared publicly

This is a must read for anyone invested in Bitcoin or people thinking of investing. The article highlights the vulnerability caused by limiting transaction capacity it could result in textbook black swan as the "Intelligent Comments" highlights.

+2 1 · Reply



Kevin Canini 6 months ago · Shared publicly

What is the economic incentive for miners to leave a chain just because other miners have left it? This seems to be a crucial part of the "spiral" you describe, but I see no explanation for it.

1 · Reply



Patrick 6 months ago

As miners leave there is less hashrate mining so the block times get longer. Longer confirmation times, longer time between block payments, users leave from transaction confirmation taking days even weeks, BTC price decrease more miners leave === thats the downward spiral feedback loop.



Shariar Porosh 2 weeks ago · Shared publicly

Liberalcoins is a local Bitcoin, Monero, Dash and Litecoin exchange. Users can directly buy and sell cryptocurrencies to each other <https://liberalcoins.com>

1 · Reply



Fanny Nicolas 3 weeks ago · Shared publicly

 Blockchain technology based casino 100 free chips. if you sign up This is probably gonna be one of the bigger, if not the biggest online casino for crypto currency

1 · Reply



Shariar Porosh 3 weeks ago · Shared publicly

<https://www.bitmex.com/register/ESkFja> > Trade Bitcoin and other cryptocurrencies with up to 100x leverage. Fast execution, low fees, Bitcoin futures and swaps: available only on BitMEX

1 · Reply



Shariar Porosh 3 weeks ago · Shared publicly



The Best Cryptocurrency Affiliate Programs.BEST BITCOIN AND CRYPTOCURRENCY EXCHANGES 2018

Cryptocurrency, Bitcoin, Ethereum, Affiliate, Referral, Program
<https://www.cryptotrust.ca>

1 · Reply



New Level Coin 1 month ago · Shared publicly

We are launching a brand new cryptocurrency - NewLevelCoin and its ICO starts on 10th Feb 2018. Kindly visit the following link to know more:
<http://newlevelcoin.co/>

1 · Reply



Robert Nash 1 month ago · Shared publicly

On January 23rd, South Korea's Financial Services Commission confirmed in a statement that all Bitcoin investors and traders would need to do future business dealings through real-name bank accounts in order to "reduce room for cryptocurrency transactions to be exploited for illegal activities, Read more (10 lines)

1 · Reply



Roland Rocke 1 month ago · Shared publicly

I am a new satisfied customer with the darkwebsolutions company, they helped me recover my investment, stolen BTC... They take care of other hack related and identity issues too. visit darkwebsolutions dott coo

+1 1 · Reply



Stock Market Tips Provider 1 month ago · Shared publicly

To make good money in stock markets, one should practice the fundamental method of investing.For more info visit CapitalHeight

1 · Reply



Dj Lakhany 3 months ago (edited) · Shared publicly

There is a lot that we need to look at when it comes to these things. We need to look back and understand how things worked, as that is what will help us most when it comes to gaining. The greatest thing happened with us was the Crypto industry with upcoming ICOs, it can be great if we spot right opportunity. And, I can't see a better bet than <https://sale.coinfi.com>, it is the superstar of the future with magnificent concept that's based upon giving us the analytic platform to help with knowing where to invest and updated with the happening, it is the future of crypto industry!

1 · Reply



Rohit Sharma 3 months ago · Shared publicly

Thankyou so much sharing for informative valuable post. Many people will profit from this post in their business Great Job, Keep it up.
<https://www.goldcruderesearch.com>

1 · Reply



Journey Time 3 months ago · Shared publicly

Raxcard.com is providing Best Bitcoin ATM Debit Card, Really nice to withdraw bitcoin money from local ATM, you can get best value of your bitcoin, we offer visa and master card for Bitcoin with free shipping.

<http://www.raxcard.com/order/>

1 · Reply

[Show more](#)

[Newer Post](#)

[Home](#)

[Older Post](#)

Subscribe to: [Post Comments \(Atom\)](#)

Followers

Mga sumusubaybay (2)



[Sundin](#)

Followers

Simple theme. Powered by [Blogger](#).